Э.В. Афонцев, соискатель
Научный руководитель: Поршнев С.В., проф., д-р. техн. наук

ИЗУЧЕНИЕ СВОЙСТВ САМОПОДОБИЯ ВРЕМЕННЫХ РЯДОВ В ЗАДАЧЕ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА

Проблема детектирования сетевых аномалий, обусловленных хакерской активностью, заражением определенными типами вирусов, а также неправильно сконфигурированным оборудованием, на сегодняшний день окончательного решения не имеет. Наиболее популярные в данный момент сигнатурные детекторы, как показывает опыт их практического использования, способны обнаружить только известные нарушения. Таким образом, разработка подходов к решению задачи выявления неизвестных сетевых аномалий остается по-прежнему актуальной.

С нашей точки зрения, несомненный интерес представляет исследование возможности использования в данной задаче методов нелинейной динамики. В частности, представляется целесообразным проверить гипотезу о связи между уровнем сетевого трафика и его фрактальной размерностью. Для оценки последней мы использовали показатель Херста H, определяемый для временного ряда $x_k, k = 1,2,\text{K}\ N$ из соотношения

$$R/S = (aN)^H, \qquad (1)$$

где $R = \max(x_k) - \min(x_k)$ – размах отклонения; $S = \sqrt{\frac{1}{N-1}\sum_{k=1}^{N}(x_k - \bar{x})^2}$ – стандартное отклонение, N – число членов временного ряда, a – константа.

Напомним, что, используя значение показателя Херста H, выделяют три типа случайных процессов: 1) $0 \le H < 0,5$ случайный процесс является антиперсистентным, или эргодическим, рядом, который не обладает самоподобием; 2) $H = 0,5$ – полностью случайный ряд, аналогичный случайным смещениям частицы при классическом броуновском движении; 3) $H > 0,5$ персистентный (самоподдерживающийся) процесс, который обладает длительной памятью и является самоподобным.

Необходимо отметить, что большинство исследователей теории сетевого трафика концентрируют свои усилия в разработке новых моделей потоков данных на основе применения свойств самоподобия, в качестве практического приложения ограничиваясь в основном методиками расчета пропускной способности сетевых каналов.

Авторами проведена работа по изучению поведения параметра Херста, определяемого в соответствии с (1), для выявления аномальной сетевой активности. Типичные примеры анализируемых временных рядов представлены на рис. 1, 2. Методику оценки показателя Херста H иллюстрируют рис. 3, 4.

Предварительный анализ зарегистрированных временных рядов показал, что сетевой трафик действительно обладает эффектом самоподобия. Параметр Херста во всех случаях превышает 0,5. Гипотеза о количественном отличии параметра Херста для независимых измерений штатного и аномального сетевого

трафика не подтвердилась. Однако в ходе экспериментов получен следующий практически важный результат: параметр Херста для трафика, содержащего аномалии, всегда больше соответствующего значения для того же трафика после удаления аномалий, которое осуществлялось удалением из файла данных пакетов, принадлежащих к ip-адресам, которые визуально определялись как относящиеся к зараженным.

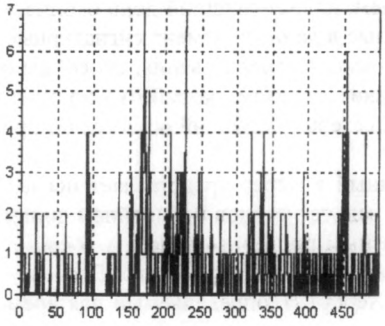

Рис. 1. Трафик с аномалиями (число пакетов/с)

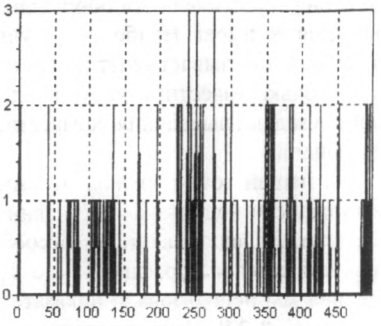

Рис. 2. Трафик с удаленными аномалиями (число пакетов/с)

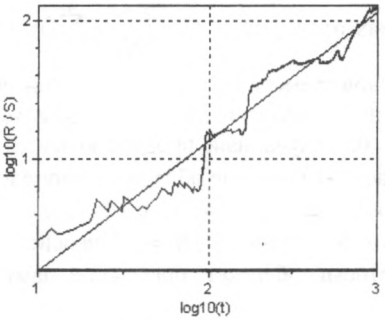

Рис. 3. Зависимость lg(R/S) от lg(t) для трафика с аномалиями, H=0.93

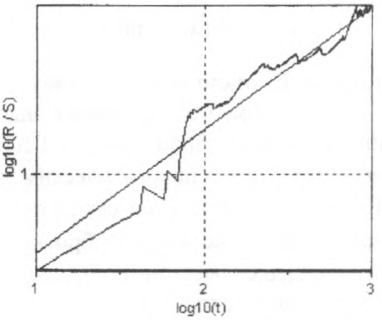

Рис. 4. Зависимость lg(R/S) от lg(t) для трафика без аномалий, H=0.67

Обнаруженный факт требует теоретического обоснования. Можно предположить, что усиление самоподобия является характерным для сетевой активности вирусных программ, выполняющих в программном цикле процедуры заражения, а также для различных сетевых сканеров. Таким образом, для надежного детектирования аномалий в сети на основе анализа свойств самоподобия требуется проведение дальнейших исследований.